PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Kohshiro INOMATA et al.

Application No.: 10/624,681

Filed: July 23, 2003 Docket No.: 116655

For: DEVICE FOR COMPRESSION AND ENCRYPTION, AND DEVICE FOR DECOMPRESSION AND DECRYPTION

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2002-367671 filed on December 19, 2002

In support of this claim, a certified copy of said original foreign application:

☒ is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

JAO:JSA/mlo

Date: December 31, 2003

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１２月１９日

出願番号
Application Number: 特願２００２－３６７６７１

[ST. 10/C]: [ＪＰ２００２－３６７６７１]

出願人
Applicant(s): 富士ゼロックス株式会社

２００３年１２月　４日

特許庁長官
Commissioner,
Japan Patent Office

今井康

出証番号　出証特２００３－３１００４２６

【書類名】　特許願
【整理番号】　FE02-01394
【提出日】　平成14年12月19日
【あて先】　特許庁長官殿
【国際特許分類】　H04N　1/41
【発明者】
　【住所又は居所】　神奈川県足柄上郡中井町境４３０　グリーンテクなかい
　富士ゼロックス株式会社内
　【氏名】　猪股　浩司郎
【発明者】
　【住所又は居所】　神奈川県足柄上郡中井町境４３０　グリーンテクなかい
　富士ゼロックス株式会社内
　【氏名】　光武　克也
【特許出願人】
　【識別番号】　000005496
　【氏名又は名称】　富士ゼロックス株式会社
【代理人】
　【識別番号】　100075258
　【弁理士】
　【氏名又は名称】　吉田　研二
　【電話番号】　0422-21-2340
【選任した代理人】
　【識別番号】　100096976
　【弁理士】
　【氏名又は名称】　石田　純
　【電話番号】　0422-21-2340
【手数料の表示】
　【予納台帳番号】　001753
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　圧縮暗号化装置及び伸長復号化装置

【特許請求の範囲】

【請求項１】　所定の参照テーブルを参照して圧縮対象データをデータ圧縮する圧縮手段と、

前記参照テーブル自体又はその参照テーブルを再構成するのに必要な情報を暗号化する暗号化手段と、

前記圧縮手段により得られた圧縮データと、前記テーブル暗号化手段により得られた暗号化データとをまとめて多重化データを作成する多重化手段と、

を備え、前記多重化データを暗号化結果として出力する圧縮暗号化装置。

【請求項２】　前記参照テーブルは、前記圧縮対象データの各周波数成分の値を量子化する際の量子化ステップサイズを定めた量子化テーブルであることを特徴とする請求項１記載の圧縮暗号化装置。

【請求項３】　前記参照テーブルは、データをエントロピー符号化する際のデータ値と符号語との関係を定めた符号化テーブルであることを特徴とする請求項１記載の圧縮暗号化装置。

【請求項４】　前記暗号化手段は、更に前記圧縮データをデータ伸長することにより得られるデータを意味あるデータとして解釈するために必要となるパラメータを暗号化することを特徴とする請求項１記載の圧縮暗号化装置。

【請求項５】　前記圧縮データから一部のデータを取り除くデータ抽出手段を更に備え、

前記暗号化手段は、更に前記データ抽出手段により前記圧縮データから取り除かれた一部のデータを暗号化し、

前記多重化手段は、前記データ抽出手段により前記一部のデータを取り除いた残りの圧縮データと、前記暗号化手段の暗号化結果とをまとめて前記多重化データを作成する、

ことを特徴とする請求項１記載の圧縮暗号化装置。

【請求項６】　前記圧縮対象データの性質及び前記データ圧縮の圧縮条件の少なくとも一方に応じて作成された参照テーブルのうち、少なくとも１つのテー

ブルエントリの値を変更する参照テーブル変更手段を更に備え、前記圧縮手段は前記参照テーブル変更手段で変更された前記参照テーブルを用いてデータ圧縮を行うことを特徴とする請求項１記載の圧縮暗号化装置。

【請求項７】　前記参照テーブルのテーブルサイズを変更する参照テーブル変更手段を更に備え、前記圧縮手段は前記参照テーブル変更手段でサイズ変更された前記参照テーブルを用いてデータ圧縮を行うことを特徴とする請求項１記載の圧縮暗号化装置。

【請求項８】　入力された多重化データから、圧縮データと暗号化データとを抽出するデータ抽出手段と、

前記暗号化データを復号することにより、データ伸長の際に参照すべき参照テーブルを求める復号化手段と、

前記参照テーブルを参照して前記圧縮データを伸長する伸長手段と、

を備え、前記伸長手段により伸長されたデータを復号結果として出力する伸長復号化装置。

【請求項９】　所定の参照テーブルを参照して圧縮対象データをデータ圧縮する圧縮ステップと、

前記参照テーブル自体又はその参照テーブルを再構成するのに必要な情報を暗号化する暗号化ステップと、

前記圧縮手段により得られた圧縮データと、前記テーブル暗号化手段により得られた暗号化データとをまとめて多重化データを作成し、出力する多重化ステップと、

を含む圧縮暗号化方法。

【請求項１０】　入力された多重化データから、圧縮データと暗号化データとを抽出するデータ抽出ステップと、

前記暗号化データを復号することにより、データ伸長の際に参照すべき参照テーブルを求める復号化ステップと、

前記参照テーブルを参照して前記圧縮データを伸長し、その伸長結果を出力する伸長ステップと、

を含む伸長復号化方法。

【請求項１１】　コンピュータシステムに、

所定の参照テーブルを参照して圧縮対象データをデータ圧縮する圧縮ステップと、

前記参照テーブル自体又はその参照テーブルを再構成するのに必要な情報を暗号化する暗号化ステップと、

前記圧縮手段により得られた圧縮データと、前記テーブル暗号化手段により得られた暗号化データとをまとめて多重化データを作成し、出力する多重化ステップと、

を実行させるためのプログラム。

【請求項１２】　コンピュータシステムに、

入力された多重化データから、圧縮データと暗号化データとを抽出するデータ抽出ステップと、

前記暗号化データを復号することにより、データ伸長の際に参照すべき参照テーブルを求める復号化ステップと、

前記参照テーブルを参照して前記圧縮データを伸長し、その伸長結果を出力する伸長ステップと、

を実行させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ圧縮とともに暗号化を行う圧縮暗号化装置、及びこれに対応する復号化装置に関する。

【０００２】

【従来の技術】

近年、デジタルカメラの普及、スキャナによるドキュメントの電子化等、画像データの利用はますます増大している。また、画像データは高精細化の傾向にあり、１画像データのデータサイズが増大する傾向にある。

【０００３】

その一方で、画像データはインターネット上の盗聴や権限の無い人に参照され

る等のデータ漏洩の危険が伴う。この対処方法として、画像データを暗号化する方法が有効である。例えば、トリプルＤＥＳやＡＥＳ等の暗号方式で暗号すれば、データの安全性は保障されると考えられている。

【０００４】

ところが、これら安全な暗号化方法の処理量はデータサイズに比例して処理時間（あるいはCPU負荷）が増大するという問題がある。復号化方法も同様である。データ数が増えればさらに処理時間が増大するのは言うまでも無い。

【０００５】

このような問題に対して、例えば特許文献１には、１画像を複数のブロックに分割し、一部のブロックのみを暗号化し、残りのブロックは暗号化したブロックとの差分を演算することによって暗号化処理量を軽減した暗号化方法が開示されている。

【０００６】

また、特許文献２には、画像データに対してＤＣＴ変換（離散コサイン変換）を行った際の直流成分のみを暗号化することによって暗号化処理量を軽減する暗号化方法が開示されている。

【０００７】

また、特許文献３には、あらかじめ設定した解析ルールに基づきデータの中の重要度が高い部分を強固な暗号手段で暗号化しそれ以外の部分については暗号強度の弱い暗号化処理を施すことによって全体の暗号化負荷を軽減する暗号化方法が開示されている。

【０００８】

【特許文献１】

特開２０００－１１５５５１公報

【特許文献２】

特開平６－１２５５５３号公報

【特許文献３】

特開２００２－１９０７９８公報

【０００９】

【発明が解決しようとする課題】

しかしながら、特許文献１に開示される方法は、たしかに暗号化処理を施すのは暗号化対象のデータの一部分のみであるが、それ以外の部分についても暗号化した部分との差分をとる演算を行わなくてはならないため、データサイズが大きいデータに対しては必ずしも全体の処理量が軽減されない。

【００１０】

また、特許文献２に開示される方法では、直流成分は全体のデータ量の一定量（通常1/64）を占めるため、データサイズに比例して暗号処理量も増加してしまうという問題がある。

【００１１】

また、特許文献３に開示される方法は、画像の各部分にあらかじめ重要度を定義してあるデータにしか適用できないため、適用できるデータが限定されてしまうという問題がある。

【００１２】

このように従来技術では、データサイズが増大すると依然として暗号処理にかかる処理量の負荷（あるいは処理時間）が増大するという問題や、未知なるフォーマットに対しては効果が無いなどの問題がある。

【００１３】

以上、画像データの暗号化を例にとったが、画像データ以外のデータについても同様の問題がある。

【００１４】

本発明は上記従来の事情に鑑みなされたものであり、膨大な量のデータを圧縮及び暗号化する場合において、低いＣＰＵ負荷又は短い所要時間で圧縮・暗号化の処理ができるようにすることを目的とする。

【００１５】

【課題を解決するための手段】

本発明では、ハフマン符号化やＪＰＥＧ、ＭＰＥＧなど、ある種の圧縮符号化方式が、符号化テーブルや量子化テーブルなど、データ圧縮処理に必要なパラメータを記憶したテーブルを用い、そのテーブルの情報を圧縮データとともに１つ

のファイルにまとめるという点に着目した。すなわち本発明では、圧縮及び暗号化したいデータそのもの（圧縮対象データと呼ぶ）を暗号化する代わりに、そのようなデータ圧縮の際に用いるデータ変換用の参照テーブルを暗号化することとした。

【００１６】

【発明の実施の形態】

以下、本発明の好適な実施の形態（以下、「実施形態」と呼ぶ）を、図面を参照して説明する。以下では、画像データを圧縮暗号化する場合を主たる例として説明する。

【００１７】

図１は、本発明の実施形態に係る圧縮暗号化装置の構成を示すブロック図である。例示する装置は、画像データを圧縮暗号化する装置である。

【００１８】

ブロック分割部１０は、圧縮対象データ（ここでは画像データ）をｎ画素×ｎ画素のデータで構成されるブロック単位に分割する。例えばＪＰＥＧ圧縮の場合、ｎ＝８である。分割された各ブロックのデータは、所定の二次元直交変換処理により、ｎ×ｎ個の周波数成分の組に変換される（図示省略）。例えばＪＰＥＧ圧縮の場合、直交変換処理としてＤＣＴ（離散コサイン変換）処理が行われる。これらｎ×ｎ個の周波数成分の組が量子化部１２に入力される。

【００１９】

量子化部１２は、入力されるｎ×ｎ個の各周波数成分の値を、量子化テーブル１４に基づいて量子化する。量子化テーブル１４は、ｎ×ｎ個の量子化閾値を含んだテーブルであり、個々のテーブルエントリ（すなわち量子化閾値）は量子化処理に先立ってあらかじめ設定されている。量子化テーブル１４としては、圧縮対象データの全ブロックに対してただ一つの量子化テーブル１４を用いてもよいし、複数の量子化テーブル１４を用い、複数ブロック毎に量子化テーブル１４を変えてもよい。なお、量子化テーブル１４を参照して行う量子化処理は、ＪＰＥＧ圧縮等で行われている一般的な処理でよい。例えば量子化処理としては、周波数成分(u,v)（u,vは０～ｎ－１の整数）の値をS_uvとし、量子化テーブル１４に

おいてこの周波数成分に対応する閾値をQ_uvとしたとき、次式で定義される式をｎ×ｎ個のデータ全てに適用し、出力データr_uvを求める処理でよい。

【００２０】

r_uv = round(S_uv / Q_uv)

ただしroundとはもっとも近い整数への整数化を意味する。

【００２１】

この量子化処理は、非可逆の処理であるが、圧縮対象データのデータサイズを大幅に削減することができる。画像データの場合、このような非可逆の圧縮により多少情報が失われても、人間の目にはその影響がわかりにくい場合が多い。

【００２２】

この処理により得られたｎ×ｎ個の量子化データが、エントロピー符号化部１６に入力される。エントロピー符号化部１６は、それら量子化データに対し、符号化テーブル１８を参照して符号化処理を施す。この符号化処理は、符号化テーブルを利用するエントロピー符号化処理であれば、基本的に何でもよい。例えばＪＰＥＧ圧縮の場合、エントロピー符号化としてハフマン符号化処理が用いられる。また、エントロピー符号化部１６では、量子化データを複数の種別に区分し、種別毎に異なるエントロピー符号化処理を施すこともできる。例えばＪＰＥＧの場合は、量子化データの直流成分と交流成分とに対し、異なる符号化処理が施される。

【００２３】

符号化テーブル１８は、量子化データの値と符号語との対応関係を示すテーブルであり、符号化処理に先立って設定されている。符号化テーブル１８としては、１つのテーブルをすべてのデータに対して適用してもよいが、データの種別毎に、その種別の性質に応じたテーブルを用意してもよい。例えばＪＰＥＧの場合、直流成分用と交流成分用とにそれぞれ符号化テーブル１８が用意される。

【００２４】

エントロピー符号化部１６は、量子化データの値に対応する符号語をこの符号化テーブル１８から求め、これを符号化結果として出力する。ｎ×ｎの１ブロックに含まれる各量子化データに対してこの符号化処理が行われる。

【００２５】

以上の量子化及びエントロピー符号化により、ブロックの圧縮データが得られる。この処理が、圧縮対象データのすべてのブロックに対して繰り返される。

【００２６】

以上の量子化及びエントロピー符号化と並行して、暗号化部２０において、量子化テーブル及び符号化テーブルの暗号化処理が行われる。この暗号化は、テーブル自体を暗号化するものでももちろんよいが、テーブルを再構成するのに必要な情報を暗号化するものでもよい。例えばＪＰＥＧの符号化テーブルの場合、周知のように、各符号長の符号語の数を示すテーブルと発生頻度順に並べた符号化要素とが分かれば、復号側で符号化テーブルを再構成できるので、それら符号語数のテーブルと発生頻度順の符号化要素のデータを暗号化しても、符号化テーブル自体を暗号化するのと同じ効果が得られる。

【００２７】

暗号化部２０で用いる暗号方式は、暗号強度が十分強い暗号方式であれば、既存の標準的な暗号方式のどれを用いてもよい。例えば公開鍵暗号方式を用いることもできるし、共通鍵暗号方式と公開鍵暗号方式を組み合わせた暗号方式を用いることもできる。

【００２８】

多重化部２４は、エントロピー符号化部１６から出力される圧縮データと、暗号化部２０から出力される量子化テーブル等の暗号化データと、復号したデータを意味あるデータとして解釈するのに必要な各種パラメータ２２とを１つに結合して、一つの多重化データにまとめる。ＪＰＥＧの場合、この多重化処理により１つのＪＰＥＧファイルができあがる。ここで圧縮対象データが画像データの場合、パラメータ２２には、例えば該画像データの全画素数、１ラインの画素数、ブロックサイズ、データ精度、コンポーネント数など、復号により得た画素データを画像情報として出力・表示するために必要となる情報が含まれる。また、このパラメータ群には、多重化データ内から暗号化データ及び圧縮データを切り分けて取り出すために必要な情報が含まれる。このような情報としては、例えば暗号化データのサイズ及び多重化データ内で暗号化データの位置（例えば、何番目

のデータセグメントが暗号化データか）などを挙げることができる。この場合、暗号化データのサイズの情報は暗号化部２０から、暗号化データの位置の情報は多重化部２４から得ることができる。

【００２９】

例えばＪＰＥＧ規格のファイルフォーマットの１つであるＪＦＩＦは、大まかに言えば、パラメータ２２、量子化テーブル１４、符号化テーブル１８、及び圧縮データの各々のフィールドがこの順に並べられ、各フィールドにはそのフィールドのデータサイズ（すなわちデータ長）の情報が含まれている。これに対し、本実施形態にて、量子化テーブル１４及び符号化テーブル１８のフィールドを暗号化してしまうと、復号側ではこれら各フィールドのデータ長の情報が見えなくなるので、どこまでが暗号化データであり、どこから先が圧縮データのフィールドなのかが分からなくなる。そこで、本実施形態では、前述のごとく、多重化データ内から暗号化データ及び圧縮データを切り分けて取り出すために必要な情報をパラメータ２２に含めることで、復号側で暗号化データと圧縮データとが抽出できるようにしている。なお、ＪＰＥＧ圧縮に本実施形態の方式を適用した場合、パラメータ２２のフィールド長は、ＪＰＥＧ規格のフォーマットの記述から分かるので、後は暗号化データのデータサイズが分かれば、圧縮データの先頭位置を求めることができ、多重化したファイルからパラメータ２２，暗号化データ，圧縮データを抽出することができる。したがって、パラメータ２２には暗号化データのサイズを組み込んでおけばよい。

【００３０】

以上、本実施形態の圧縮暗号化装置について説明した。この装置によれば、暗号化するのは量子化テーブル１４と符号化テーブル１８だけであり、ＪＰＥＧ圧縮の場合、これらテーブルは両者合わせても４００バイトにも満たない小さいデータであり、圧縮対象の画像データに比べて遙かに小さい。さらに、圧縮対象データのデータサイズが大きくなってもそれらテーブルのサイズは不変である。したがって、量子化テーブル１４及び符号化テーブル１８の暗号化処理に必要なＣＰＵ能力や時間はきわめて小さい。例えば画像のＪＰＥＧ圧縮の場合、本実施形態の手法によれば、データサイズが１Mbyteの画像データであれば約1/2000、10M

byteのデータであれば約1/20000に暗号化処理量を減らすことができる。

【００３１】

そして、量子化テーブル１４や符号化テーブル１８がなければ圧縮データを正しく復号することができないので、仮に多重化データが漏洩したとしても、それらテーブルが暗号化されていれば、圧縮対象データを秘匿することができる。

【００３２】

このように、本実施形態の圧縮暗号化装置によれば、従来より少ないＣＰＵ負荷又は時間でデータの圧縮及び暗号化が可能になる。

【００３３】

この圧縮暗号化装置で作成された多重化データを伸長し復号する伸長復号化装置の構成の一例を図２に示す。

【００３４】

伸長復号化装置において、多重分離部３０は、入力される多重化データを、復号結果を意味あるデータとして解釈するために必要なパラメータ２２と、圧縮対象データを圧縮符号化した圧縮データと、量子化テーブル１４及び符号化テーブル１８を暗号化した暗号化データとに分離する。パラメータ２２は多重化データのヘッダ部分に含まれるので、このヘッダ部分から取り出すことができる。取り出したパラメータ２２には、暗号化データのサイズや位置を示す情報が含まれているので、多重分離部３０は、このパラメータに基づいて多重化データから暗号化データを取り出すことができる。多重化データからパラメータ２２と暗号化データを取り除いた残りが圧縮データである。

【００３５】

暗号復号化部３２は、抽出された暗号化データを復号して量子化テーブル１４及び符号化テーブル１８を復元する。テーブル自体が暗号化されている場合は、単に復号化するだけでそれらテーブルが復元できる。一方、暗号化データがテーブルを再構成するのに必要な情報を暗号化したものである場合、暗号復号化部３２は、暗号化データの復号結果に基づき符号化テーブル等を作成する。

【００３６】

エントロピー復号化部３４は、復元された符号化テーブル１８を参照して、圧

縮データを１ブロックずつエントロピー復号化する。この復号処理は符号化処理と逆過程の処理でよく、公知の復号処理を用いればよい。

【００３７】

逆量子化部３６は、エントロピー復号化されたブロックデータに対し、復元された量子化テーブル１４を用いて逆量子化を行う。この逆量子化処理も公知の処理を用いることができる。

【００３８】

これらエントロピー復号化部３４及び逆量子化部３６で１ブロック分の圧縮データを処理することにより、圧縮対象データ１ブロック分が再生される。ブロック合成部３８は、再生された各ブロックのデータを、パラメータ２２を参照して合成することで、圧縮対象データを再生する。

【００３９】

以上、本実施形態の圧縮暗号化装置及びこれに対応する伸長復号化装置について説明した。以上に例示した装置では、量子化テーブル１４及び符号化テーブル１８の両方を暗号化したが、いずれか一方を暗号化する構成でも、同様の効果が期待できる。

【００４０】

次に、上記実施形態の圧縮暗号化装置の第１の変形例を、図３を参照して説明する。図３において、図１に示した装置の構成要素と同一又は類似の構成要素には、同一符号を付してその説明を省略する。

【００４１】

図３に示したように、この第１の変形例では、暗号化部２０ａが、量子化テーブル１４及び符号化テーブル１８に加え、復号したデータを意味あるものとして解釈するために必要なパラメータ２２をも暗号化する。これにより、パラメータ２２も秘匿されるので、暗号化の強度をより高めることができる。

【００４２】

ただし、この変形例では、多重化データから暗号化データと圧縮データを分別して取り出すのに必要な情報（例えば暗号化データのデータサイズ）だけは、暗号化せずに復号側に渡す必要がある。逆に言えば、この変形例では、この情報以

外のパラメータ２２の全項目又は一部の項目を暗号化することができる。

【００４３】

第１の変形例に対応する伸長復号化装置（図示省略）は、暗号復号化部３２の復号化結果からパラメータ２２を抽出する以外は、図２に示した装置構成と同様でよい。

【００４４】

次に図４及び図５を参照して、第２の変形例を説明する。図４はこの変形例に係る圧縮暗号化装置の構成を示す図である。図４において、図１に示した装置の構成要素と同一又は類似の構成要素には、同一符号を付してその説明を省略する。

【００４５】

この第２変形例の圧縮暗号化装置は、図１の実施形態の構成に加え、エントロピー符号化部１６から出力される圧縮データから一部を抽出するデータ抽出部２８を更に備える。データ抽出部２８は、圧縮データからその一部のデータを取り除き、後段の多重化部２４に入力する。また、暗号化部２０ｂは、量子化テーブル１４及び符号化テーブル１８に加え、パラメータ２２とデータ抽出部２８で抽出した圧縮データの一部を暗号化し、暗号化データを生成する。そして、多重化部２４は、この暗号化データと、一部が欠落した圧縮データとを多重化する。ただし、この変形例でも、多重化データから暗号化データと圧縮データを分別して取り出すのに必要な情報（例えば暗号化データのデータサイズ）だけは、暗号化せずに多重化データに含める。

【００４６】

この変形例によれば、圧縮データの一部も秘匿されるため、暗号化の強度が向上する。例えば、仮に攻撃者が多重化データから圧縮データのみを抽出し、その圧縮データのパターンを解析して復号しようとしても、その圧縮データには欠落部分があり、しかもその欠落部分がどの部分なのかが分からないので、そのような解析はきわめて困難である。

【００４７】

この変形例では、圧縮データから欠落させる部分のデータサイズを圧縮対象デ

ータのデータサイズに応じて変えなくても、上述の暗号強度向上の効果は得られる。

【００４８】

また、この変形例では、圧縮データから欠落させる部分の位置やサイズを圧縮対象データごとに変えるようにすることもできる。これにより、暗号強度をより高めることができる。これには、例えば、圧縮暗号化処理全体を制御する制御部（図示省略）が、圧縮対象データの圧縮暗号化処理を開始する際に例えば乱数を発生させ、この乱数に従って欠落部分の位置やサイズを決定し、データ抽出部２８にこれらを指示すればよい。このとき、欠落部分の位置やサイズの情報をパラメータの一つとして暗号化し、暗号化データに組み込む。

【００４９】

なお、欠落部分の位置とサイズのどちらか一方のみを変化させる方式でも効果がある。

【００５０】

また、この変形例において、圧縮データ中の互いに離れた複数の場所からそれぞれデータを欠落させることももちろん可能である。

【００５１】

図４の圧縮暗号化装置に対応する伸長復号化装置の構成例を図５に示す。図５において、図２に示した装置の構成要素と同一又は類似の構成要素には、同一符号を付してその説明を省略する。

【００５２】

図５の伸長復号化装置では、暗号復号化部３２ａが多重化データの中の暗号化データを復号化し、量子化テーブル１４，符号化テーブル１８，パラメータ２２，及び圧縮データから欠落させたデータ部分を求める。データ合成部３９は、その欠落部分のデータを、多重分離部３０から出力される圧縮データ（欠落あり）と合成して、元の圧縮データを復元する。このとき、データ合成部３９は、暗号復号化部３２ａで復号化されたパラメータに含まれる欠落部分の位置やサイズの情報に基づき、一部欠落した圧縮データのしかるべき位置にその欠落部分を組み込むことで、圧縮データを復元する。圧縮データが復元された後は、図２の装置

と同様の処理を行えばよい。

【００５３】

なお、第２変形例では、暗号化部２０ｂは、量子化テーブル１４，符号化テーブル１８，パラメータ２２，及び圧縮データから欠落させたデータ部分を暗号化したが、量子化テーブル１４及び符号化テーブル１８の少なくとも一方と、圧縮データから欠落させたデータ部分とを暗号化する構成も可能である。

【００５４】

次に、図６を参照して、第３の変形例を説明する。図６は、この変形例に係る圧縮暗号化装置の構成を示す図である。図６において、図１に示した装置の構成要素と同一又は類似の構成要素には、同一符号を付してその説明を省略する。

【００５５】

この第３変形例は、図１の装置構成に加え、テーブル管理部４０を更に備える。テーブル管理部４０は、量子化テーブル１４及び符号化テーブル１８の少なくとも一方の内容を変更する機能を備える。

【００５６】

例えばデジタルスチルカメラでは、基礎となる量子化テーブルを備え、この基礎テーブルの各量子化閾値の値を、ユーザの圧縮率指定に応じたＱ値（品質係数）で除することで、圧縮処理の際に参照する量子化テーブルを作成することが一般的である。また、このような基礎テーブルを圧縮対象の画像データのシーンごとに個別に備え、そのシーンに応じた基礎テーブルを用いるものも知られている。しかし、いずれにしても、カメラが圧縮に用いる量子化テーブルの種類はさほど多くない。

【００５７】

したがって、暗号化データが解読できなくても、例えば使用される可能性の高い量子化テーブルの候補を総当たりで適用すれば、良好な復号結果が得られる可能性もある。

【００５８】

これに対し、この第３変形例では、圧縮率の指定やシーンの性質のなどに基づいて作成された量子化テーブル内の量子化閾値の一部又は全部の値を、テーブル

管理部４０により変更することで、使用される量子化テーブルの範囲を広げることができ、総当たり攻撃の成功率を減らすことができる。

【００５９】

ここで量子化テーブル内の閾値を大きくする方向に変更すると画質劣化を招くので、画質劣化を避けたい構成では、閾値を小さくする方向に変更することが必要である。この場合、データの圧縮率は劣化するが、暗号の安全性は高まる。

【００６０】

また、テーブル管理部４０が、量子化テーブルの変更処理を行う際、そのテーブル内の閾値のうち値を変更するものやその数をランダムに決定するようにすれば、使用される量子化テーブルのバリエーションが多くなって好ましい。また、閾値の変更量や変更割合などをその都度ランダムに変えることも好適である。

【００６１】

テーブル管理部４０による量子化テーブルの変更処理は、毎回の圧縮暗号化処理ごとや、圧縮暗号化処理を複数回行うごとなど、所定の規則に従って定まるタイミング毎に行えばよい。

【００６２】

以上、テーブル管理部４０により量子化テーブル１４の内容を動的に変更する例を説明したが、同様の方法で符号化テーブル１８を動的に変更することも可能である。

【００６３】

次に、図７を参照して、第４の変形例を説明する。図７は、この変形例に係る圧縮暗号化装置の構成を示す図である。図７において、図１に示した装置の構成要素と同一又は類似の構成要素には、同一符号を付してその説明を省略する。

【００６４】

この第４変形例の圧縮暗号化装置は、図１の装置構成に加え、テーブル管理部４０ａを更に備える。このテーブル管理部４０ａは、量子化テーブル１４及び符号化テーブル１８の少なくとも一方のテーブルサイズを変更する機能を備える。

【００６５】

ここで、テーブルサイズとは、テーブルのエントリ（項目欄）の数のことであ

る。例えば量子化テーブル１４には、ブロック分割部１０における圧縮対象データのブロックのサイズ、すなわち「ｎ×ｎ」に対応して、ｎ×ｎのエントリが存在する。すなわち、量子化テーブル１４のサイズはｎの値で決まる。同様に、符号化テーブルの場合、テーブルサイズは、例えば使用する符号語長の幅や、各語長で用いる符号語の数で決まる。

【００６６】

また、テーブルサイズの変更は、例えばあらかじめ各サイズのテーブルをそれぞれ用意しておき、それらテーブルの中から使用するものを選択することにより実現できる。例えば、量子化テーブル１４のサイズを変更する場合、８×８ブロック用のテーブル、９×９ブロック用のテーブル、１０×１０ブロック用のテーブル、・・・と言った具合に、テーブルサイズ毎に１つ又は複数の量子化テーブルをそれぞれ用意しておけばよい。そして、所定の規則に基づき決定されるテーブル変更タイミング毎に、それらの用意した複数のテーブルの中から圧縮処理に用いるテーブルを選択することで、「テーブルサイズの変更」を実現できる。符号化テーブルのサイズ変更も、同様に、あらかじめサイズの異なる符号化テーブルを複数用意しておき、その中から使用するものを動的に決定することで、実現できる。

【００６７】

テーブル変更タイミングは、例えば、圧縮対象データの圧縮処理ごとや、圧縮処理を所定数回行うごとなど、所定の規則に基づき自動決定すればよい。

【００６８】

テーブル管理部４０ａは、このようなテーブル変更タイミングごとに、量子化テーブル１４及び符号化テーブル１８のサイズを、ランダムに又は所定のサイズ変更規則に従って決定する。そして保持している各サイズのテーブルの中からそのサイズのものを選んで量子化部１２及びエントロピー符号化部１６に提供する。また、テーブル管理部４０ａは、量子化テーブル１４のテーブルサイズ、すなわちｎの値をブロック分割部１０に提供する。ブロック分割部１０は、このｎの値に応じてブロックサイズを設定し、圧縮対象データをｎ×ｎ画素のブロックに分割する。ここで、必要に応じて、各テーブル１４及び１８のテーブルサイズを

示す情報をパラメータ２２の一部として多重化データに組み込むことも可能である。これにより、復号側でそれらテーブルを正しく復元することができる。このテーブルサイズの情報を暗号化した上で多重化データに組み込めば、データ漏洩時の安全性を高めることができる。

【００６９】

ここでは、量子化テーブル１４と符号化テーブル１８の両方のサイズを変更する場合を例示したが、一方のみをサイズ変更する構成でも効果がある。また、テーブルサイズの変更に加え、前記第３変形例と同様に、選択したテーブルの中の一部又は全部のエントリの値を動的に変更することも可能である。これにより、更に暗号強度を高めることができる。

【００７０】

第４変形例の圧縮暗号化装置によれば、量子化テーブル１４及び符号化テーブル１８のうち少なくとも一方のテーブルサイズを動的に変更するので、攻撃者がそれらテーブルを推定することが困難となる。これにより暗号強度が向上する。

【００７１】

なお、第４変形例の圧縮暗号化装置に対応する伸長復号化装置は、復号化により復元した量子化テーブル１４のテーブルサイズに合わせて、ブロック合成におけるブロックサイズを設定する構成とすればよい。

【００７２】

【発明の効果】

以上説明してきたように、上記実施形態及び各変形例によれば、例えば価格や携帯性などの理由からＣＰＵ性能やメモリ量などに制約がある場合でも、暗号化に必要となる処理量（処理時間）が少なくなるので、セキュアかつ実用的なサービスが実現可能となる。

【００７３】

以上に説明した実施形態及び各変形例の圧縮暗号化装置及び伸長復号化装置は、プログラムを用いてソフトウエア的に実現することもできるし、その一部又は全部をハードウエア回路化することも可能である。

【００７４】

以上、画像データの圧縮を例にとって説明したが、本発明の手法は、動画像データやテキストデータなどの各種データに適用可能である。また、本発明の手法は、ＪＰＥＧ圧縮以外にも、ＭＰＥＧ圧縮やハフマン符号化など、圧縮処理のために符号化テーブル等の変換テーブルを用いる各種圧縮方式に適用可能である。

【図面の簡単な説明】

【図１】　実施形態の圧縮暗号化装置の構成を示す機能ブロック図である。

【図２】　実施形態の伸長復号化装置の構成を示す機能ブロック図である。

【図３】　第１変形例の圧縮暗号化装置の構成を示す機能ブロック図である。

【図４】　第２変形例の圧縮暗号化装置の構成を示す機能ブロック図である。

【図５】　第２変形例の伸長復号化装置の構成を示す機能ブロック図である。

【図６】　第３変形例の圧縮暗号化装置の構成を示す機能ブロック図である。

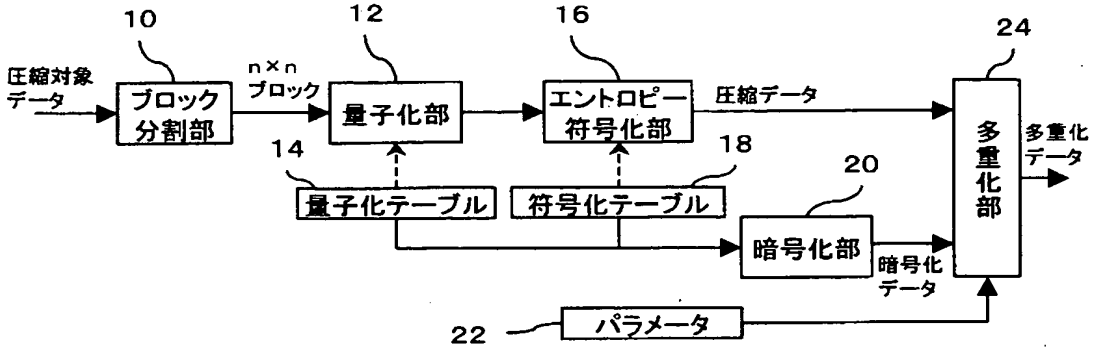
【図７】　第４変形例の圧縮暗号化装置の構成を示す機能ブロック図である。

【符号の説明】

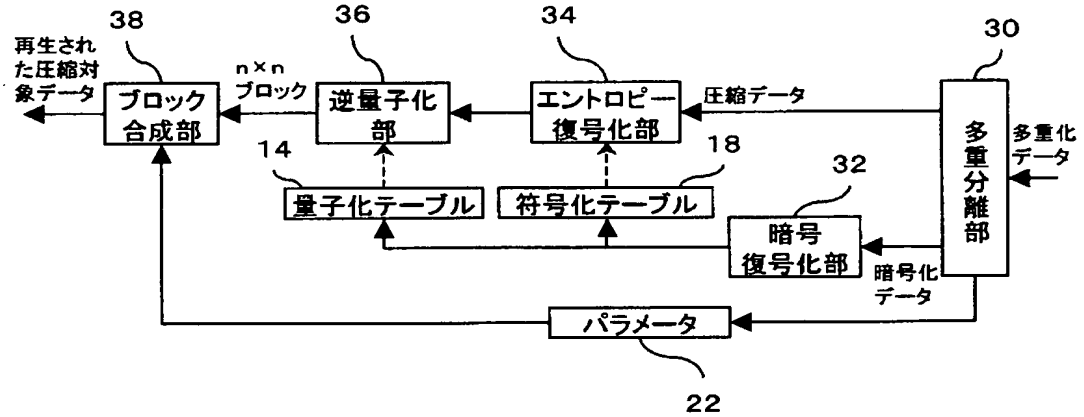
１０　ブロック分割部、１２　量子化部、１４　量子化テーブル、１６　エントロピー符号化部、１８　符号化テーブル、２０　暗号化部、２２　パラメータ、２４　多重化部。

【書類名】　図面

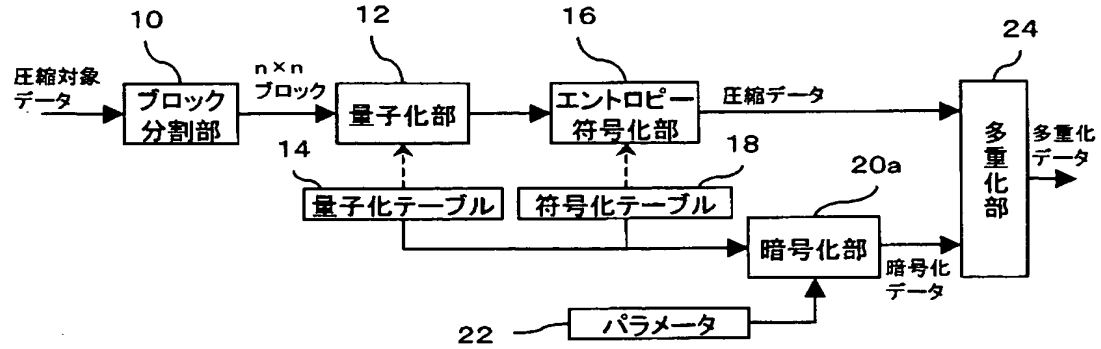
【図１】



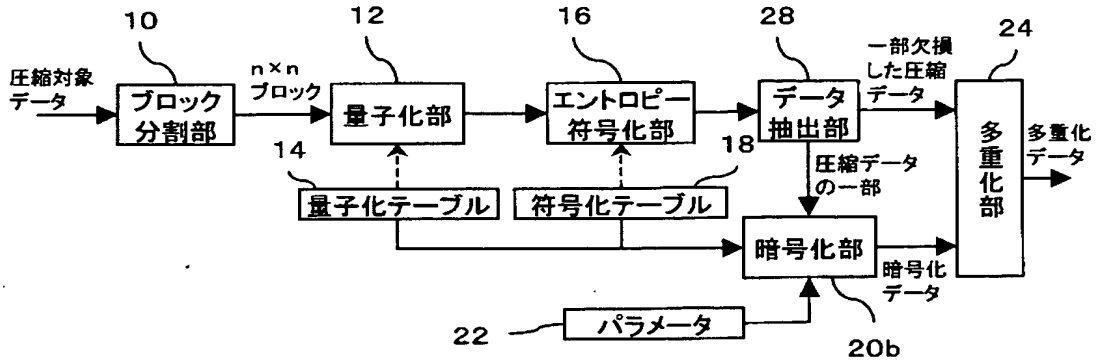
【図２】



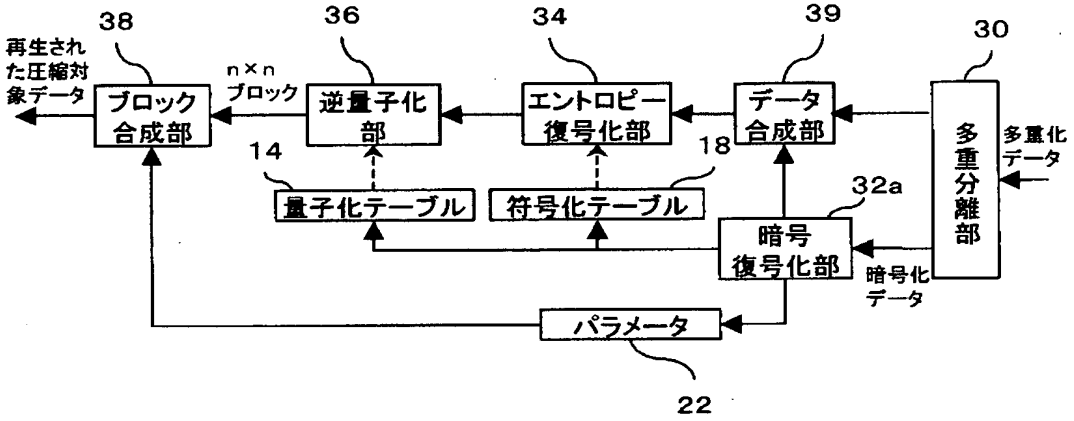
【図３】



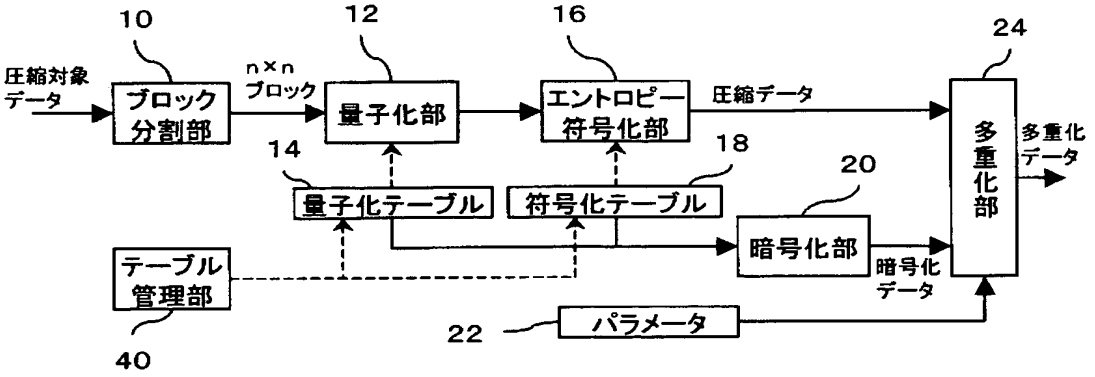
【図４】


10
12
16
28
24
圧縮対象データ
ブロック分割部
n×n ブロック
量子化部
エントロピー符号化部
データ抽出部
一部欠損した圧縮データ
多重化部
多重化データ
14
18
量子化テーブル
符号化テーブル
圧縮データの一部
暗号化部
暗号化データ
22
パラメータ
20b

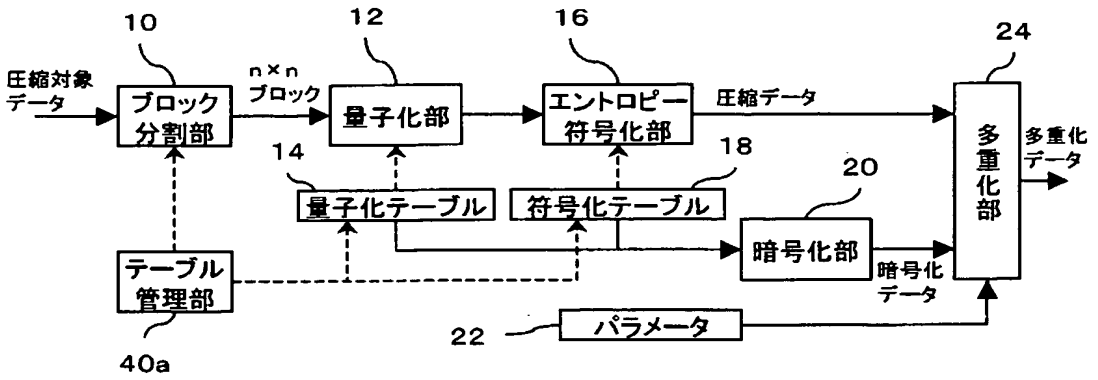
【図５】


38
36
34
39
30
再生された圧縮対象データ
ブロック合成部
n×n ブロック
逆量子化部
エントロピー復号化部
データ合成部
多重分離部
多重化データ
14
18
32a
量子化テーブル
符号化テーブル
暗号復号化部
暗号化データ
パラメータ
22

【図６】


10
12
16
24
圧縮対象データ
ブロック分割部
n×n ブロック
量子化部
エントロピー符号化部
圧縮データ
多重化部
多重化データ
14
18
20
量子化テーブル
符号化テーブル
暗号化部
暗号化データ
テーブル管理部
40
22
パラメータ

【図７】


10
12
16
24
圧縮対象データ
ブロック分割部
n×n ブロック
量子化部
エントロピー符号化部
圧縮データ
多重化部
多重化データ
14
量子化テーブル
18
符号化テーブル
20
暗号化部
暗号化データ
テーブル管理部
40a
22
パラメータ

【書類名】　　要約書

【要約】

【課題】　データの圧縮及び暗号化に必要な処理負荷又は処理時間を低減する。

【解決手段】　画像データ等の圧縮対象データは、ブロック分割部１０により所定のブロックサイズに分割される。それら各ブロックのデータを、量子化部１２が量子化テーブル１４を参照して量子化する。この量子化結果を、エントロピー符号化部１６が符号化テーブル１８を参照して符号化することで、圧縮データが得られる。暗号化部２０は、以上の量子化、符号化に用いた量子化テーブル１４及び符号化テーブル１８を所定の暗号方式で暗号化する。多重化部２４は、この結果得られた暗号化データを、圧縮データとともに所定のフォーマットにまとめる。

【選択図】　　図１

特願２００２－３６７６７１

出　願　人　履　歴　情　報

識別番号　　［０００００５４９６］

１．変更年月日　　１９９６年　５月２９日
［変更理由］　　住所変更
住　所　　東京都港区赤坂二丁目１７番２２号
氏　名　　富士ゼロックス株式会社